IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

VANDERBILT UNIVERSITY,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No. 3:18-cv-00046**
	)	
	)	**Chief Judge Waverly D. Crenshaw, Jr.**
SCHOLASTIC, INC., HOUGHTON MIFFLIN HARCOURT PUBLISHING COMPANY, and TED S. HASSELBRING,	)	**Magistrate Judge Jeffery S. Frensley**
	)	
Defendants.	)	

VANDERBILT'S MEMORANDUM IN SUPPORT OF
ITS MOTION FOR PROTECTIVE ORDER

INTRODUCTION

Vanderbilt University, as a higher education institution and an employer, maintains certain information technology ("IT") policies regarding the use of its IT systems and equipment ("Vanderbilt's systems"). Most notably, Vanderbilt has an Acceptable Use Policy that warns individuals using its systems that they "should not expect that records created, stored or communicated with [Vanderbilt's systems] … will necessarily be private." Vanderbilt further provides a "Notice to Users" to those individuals who access Vanderbilt's secure network via Vanderbilt's VPN (*i.e.*, Vanderbilt's virtual private network). This Notice to Users similarly warns individuals that they "HAVE NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY" and provides individuals access to the Acceptable Use Policy.

Vanderbilt's Acceptable Use Policy is in its Faculty Manual, provided to all Vanderbilt faculty, and published on the internet. The Acceptable Use Policy provides, "All members of the Vanderbilt University community are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy." Vanderbilt's Notice to Users is shown to every individual accessing the Vanderbilt network remotely through the Vanderbilt VPN and requires those individuals to affirmatively assent to Vanderbilt's policies before accessing the network by clicking a "Proceed" button.

Defendant Ted S. Hasselbring is an emeritus faculty member at Vanderbilt. While serving as a regular faculty member (*i.e.*, before taking emeritus status), Hasselbring received Vanderbilt's Acceptable Use Policy in Vanderbilt's Faculty Manual and would have been on notice of the Acceptable Use Policy. Hasselbring has admitted that the Faculty Manual constituted part of his contractual relationship with Vanderbilt. (Dkt. No. 129 ¶ 19; *see also id.* ¶ 7, Counterclaim.) Even beyond that admission, the Acceptable Use Policy's publication provided sufficient notice to Hasselbring of his lack of privacy in Vanderbilt's systems. Vanderbilt's records also reveal that Hasselbring accessed Vanderbilt's network through the Vanderbilt VPN at least twelve times between September 2017 and April 2018. To access Vanderbilt's network through the VPN, Hasselbring had to have reviewed the Notice to Users, seen Vanderbilt's warning as to the lack of any expectation of privacy when using Vanderbilt's systems, learned that Vanderbilt may monitor his use or data on its systems, acknowledged his awareness of the Acceptable Use Policy, and nevertheless consented to such monitoring and no expectation of privacy.

With that notice and acknowledgment of Vanderbilt's policies, Hasselbring accessed Vanderbilt's systems. As a result, Vanderbilt now possesses documents created and used by

Hasselbring while on Vanderbilt's systems. Upon realizing that it possessed those documents, Vanderbilt sequestered documents that could potentially be privileged via an initial privilege screen. The privilege screen identified 229 documents that could potentially be privileged. No member of Vanderbilt's litigation counsel in this action (the "Vanderbilt Legal Team") has reviewed those documents. An additional 578 documents that could potentially be privileged were flagged by an off-shore review team (the "Contract Reviewers") while reviewing the documents, and, again, no member of the Vanderbilt Legal Team has reviewed those documents. Instead, out of an abundance of caution, Vanderbilt's Legal Team used an independent reviewer to determine which, if any, of the 807 documents identified by the privilege screen and the Contract Reviewers were arguably privileged, without consideration of their storage on Vanderbilt's systems or Vanderbilt's IT policies. The independent reviewer identified 237 arguably privileged documents (the "Relevant Documents"). The Relevant Documents are the subject of this Motion.

Under the well-established case law in this Circuit, Hasselbring has waived any otherwise applicable privilege in the Relevant Documents. Courts examining waiver in similar circumstances apply the four factors recognized in *In re Asia Global Crossing Ltd.*: (1) did the employer maintain a policy banning personal or other objectionable use; (2) does the employer monitor employee's use or electronic transactions; (3) do third parties have the right to access the employee's records; and (4) did the employer notify the employee, or was the employee aware, of the employer's policies. 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005). The four *Asia Global* factors are satisfied here. First, Vanderbilt's Acceptable Use Policy and Notice to Users provide that Vanderbilt's systems should only be used for their "intended purposes" and warns about the consequences of misuse. Second, those policies warn that Vanderbilt has the ability to monitor computer use and electronic transactions. Third, Vanderbilt's policies allowed for third parties,

including Vanderbilt, to access employees' records. Finally, Hasselbring received notice and was aware of Vanderbilt's policies via Vanderbilt's Faculty Manual, the Acceptable Use Policy's online publication, and the Notice to Users, which Hasselbring acknowledged acceptance of twelve times. Therefore, Hasselbring waived any privilege applicable to the Relevant Documents.

In sum, the Court should grant Vanderbilt's Motion for Protective Order and enter an Order ruling that the Relevant Documents are not privileged because any privilege potentially applicable to the Relevant Documents has been waived by Hasselbring.

FACTUAL BACKGROUND

I. Vanderbilt's Acceptable Use Policy, Notice to Users, and CrashPlan Application.

Much like any other higher education institution or employer, Vanderbilt has a number of IT policies in place regarding the operation of its IT systems and equipment – Vanderbilt's systems. (Sayeed Ehsan Sidiqyar Decl. ¶ 2 (Exhibit A).) One of Vanderbilt's policies is its Acceptable Use Policy. (*Id.* ¶ 3 (attaching Acceptable Use Policy as Exhibit 1).) In place since August 2012, the Acceptable Use Policy is accessible via Vanderbilt's website and also part of the Faculty Manual provided to Vanderbilt faculty. (*Id.* ¶¶ 4-5, 9.) In relevant part, the Acceptable Use Policy states that all users of Vanderbilt's systems are on notice of the policy given its publication:

> This policy applies to all Vanderbilt University students, faculty and staff and to all others granted use of Vanderbilt's information technology (IT) resources whether individually controlled or shared, stand-alone or networked…. All members of the Vanderbilt University community are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All users are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of the University's IT resources.

(*Id.* ¶ 6.) As a member of Vanderbilt's faculty, Hasselbring would have been on notice of Vanderbilt's Acceptable Use Policy. Moreover, Vanderbilt's offer of employment to Hasselbring

explicitly stated that the policies set forth in the Faculty Manual constitute part of the contractual relationship between Hasselbring and the University. Hasselbring signed the letter, indicating his agreement. And, in fact, Hasselbring has admitted in this litigation that the Faculty Manual containing the Acceptable Use Policy was part of his contractual relationship with Vanderbilt. (Dkt. No. 129 ¶ 19; *see also id.* ¶ 7, Counterclaim (alleging that the Faculty Manual was an enforceable part of his employment agreement).)

The Acceptable Use Policy further provides that Vanderbilt may obtain the records or electronic transactions of students, faculty, and staff who use its systems:

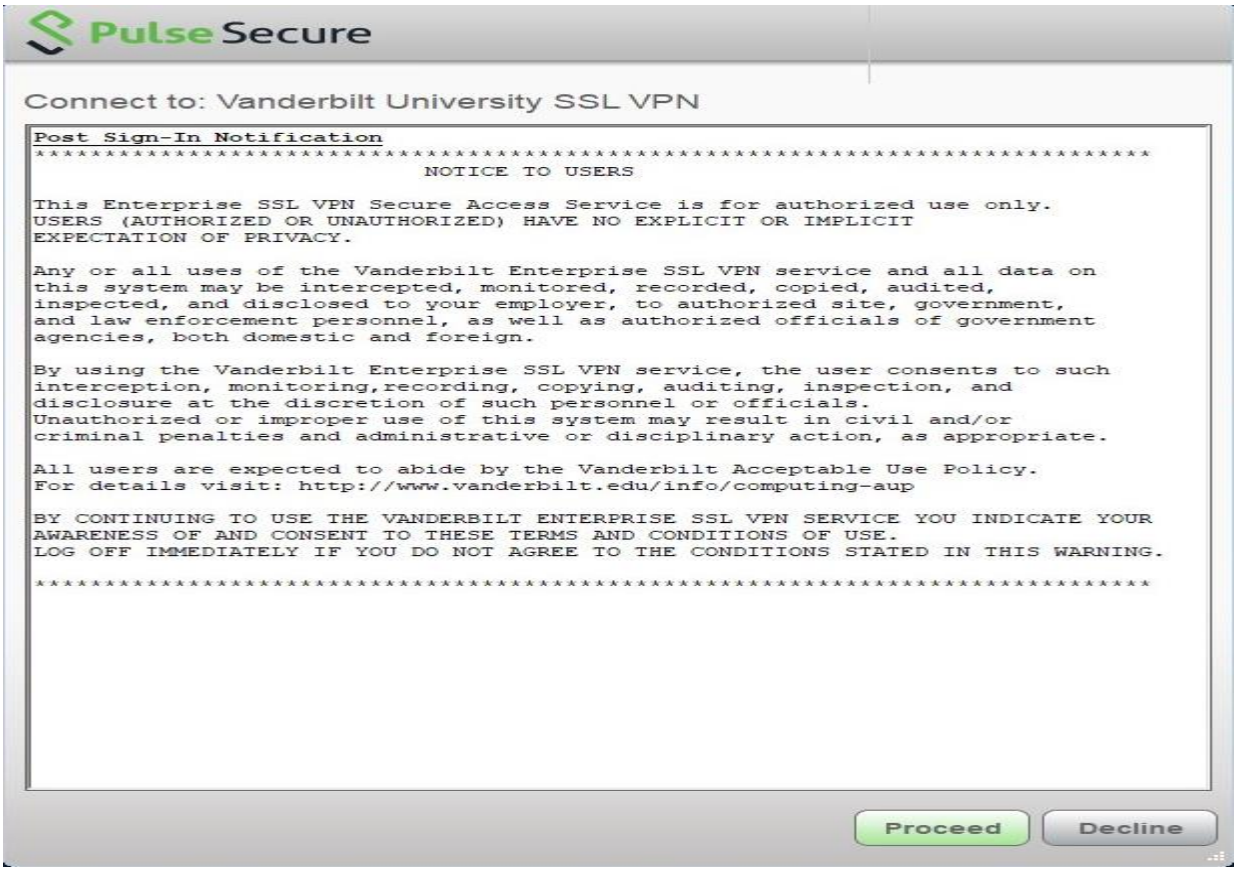
> Vanderbilt University reserves the right to obtain copy and convey to outside persons any records or electronic transactions completed using [Vanderbilt's systems] in the event it is required by law or institutional policy to do so. Vanderbilt University may also in its reasonable discretion, when circumstances require, obtain and review any records relevant to an internal investigation concerning compliance with Vanderbilt University rules or policies applicable to students, faculty, staff, or to all others granted use of Vanderbilt's information technology resources. Users therefore should not expect that records created, stored or communicated with [Vanderbilt's systems] … will necessarily be private.

(Sidiqyar Decl. ¶ 7.) Therefore, Vanderbilt faculty, including Hasselbring, were on notice that Vanderbilt could access records on its systems and that such records could not be considered private.

In addition to Vanderbilt's Acceptable Use Policy, Vanderbilt provides a "Notice to Users," containing Vanderbilt's IT policies and warning that no expectation of privacy exists. (*Id.* ¶ 10.) Vanderbilt provides the Notice to Users to those individuals (*i.e.*, "users") who remotely access certain secure applications on Vanderbilt's secure network (the "Vanderbilt network"). (*Id.*) Remote access to the Vanderbilt network occurs through the Vanderbilt University SSL Virtual Private Network (the "Vanderbilt VPN"). (*Id.*) When a user attempts to connect to the Vanderbilt network through the Vanderbilt VPN, the user must first verify their credentials. (*Id.* ¶ 11.) After verification of their credentials, the user will receive a "Notice to Users" that appears

on their computer or laptop screen. (*Id.* ¶ 12.) Every user accessing the Vanderbilt network remotely through the Vanderbilt VPN will receive the Notice to Users after the credential verification process. (*Id.* ¶ 12.) No user accessing the Vanderbilt network through the Vanderbilt VPN can bypass the Notice to Users, and the Notice to Users has been in place since at least September 17, 2017. (*Id.* ¶¶ 12-13.)

The Notice to Users explains Vanderbilt's policies to users. It warns users that they do not have any expectation of privacy when using Vanderbilt's systems. (*Id.* ¶ 15.) The Notice to Users further warns users that Vanderbilt may intercept, monitor, record, copy, audit, inspect, or disclose (to certain other third parties) any uses or data on its systems. (*Id.*) It also states that all users are expected to abide by the Vanderbilt Acceptable Use Policy. (*Id.*) In full, the Notice to Users appears as follows:



(*Id.* ¶ 14 (attaching Notice to Users as Exhibit 2).) As displayed, the Notice to Users requires the user to click a button titled "Proceed." (*Id.* ¶ 16.) The Notice to Users states, "BY CONTINUING TO USE [the Vanderbilt VPN] YOU INDICATE YOUR AWARENESS AND CONSENT TO THESE TERMS AND CONDITIONS OF USE." (*Id.*) Vanderbilt's Notice to Users instructs users to log off immediately if they do not agree to its terms. (*Id.*) Next to the button titled "Proceed" is a button titled "Decline," if a user determines that they do not consent to Vanderbilt's policies outlined in the Notice to Users. (*Id.*)

Using the username "hasselts," Hasselbring accessed Vanderbilt's network using the Vanderbilt VPN twelve times between September 17, 2017, when the Notice to Users was incorporated into the Vanderbilt VPN, and April 11, 2018. (*Id.* ¶ 19.) Therefore, on at least twelve separate occasions, Hasselbring reviewed the Notice to Users, saw Vanderbilt's warning about the lack of any expectation of privacy when using Vanderbilt's systems, learned that Vanderbilt may monitor his use or data on its systems, acknowledged his awareness of the Acceptable Use Policy, and nevertheless consented to such monitoring and lack of privacy. (*Id.*)

In line with its Notice to Users and Acceptable Use Policy, Vanderbilt uses an application called "CrashPlan" to copy and store data on Vanderbilt's systems. Vanderbilt installs CrashPlan on each computer and laptop it issues and has done so since June 2016. (*Id.* ¶ 20.) CrashPlan provides exact copies of documents on a user's Vanderbilt machine and allows for the remote copying, archiving, and retrieval of documents on the Vanderbilt-issued computer. (*Id.* ¶ 22.) For that remote retrieval and copying to occur on a user's computer, the computer must be connected to the internet. (*Id.* ¶ 23.) Upon retrieval and copying, CrashPlan keeps the copied documents in cloud storage. (*Id.* ¶ 24.) Vanderbilt's records confirm that the CrashPlan application was installed on two of its computers issued to Hasselbring. (*Id.* ¶ 21.) The CrashPlan application

made copies of Hasselbring's documents between September 20, 2016, and June 4, 2019. (*Id.* ¶ 25.)

II. Discovery of the Relevant Documents Retrieved from Hasselbring's Computers.

During the course of discovery in this litigation between Vanderbilt and Hasselbring, Vanderbilt learned that Hasselbring never returned at least two Vanderbilt-owned computers issued to him when he was a regular faculty member. (Paige Waldrop Mills Decl. ¶ 3 (Exhibit B).) While attempting to gather more information about its missing computers, Vanderbilt's counsel learned that the missing computers issued to Hasselbring had accessed Vanderbilt's VPN using Hasselbring's username – hasselts – between October 19, 2017, and April 11, 2018. (*Id.* ¶ 7.) As with all computers issued by Vanderbilt, the missing computers that Vanderbilt issued to Hasselbring contained the CrashPlan application, and so exact copies of documents on those computers had been made and stored using CrashPlan (the "Hasselbring Backups"). (*Id.* ¶ 9.)

After learning of the Hasselbring Backups, Vanderbilt's Office of the General Counsel asked Vanderbilt IT personnel to retrieve the Hasselbring Backups and copy them to a hard drive for review by Vanderbilt's litigation counsel at Bass, Berry & Sims (the "Vanderbilt Legal Team"). (*Id.* ¶ 10; *see also* Sidiqyar Decl. ¶ 25.) Vanderbilt IT personnel retrieved the Hasselbring Backups and provided them to Vanderbilt's Office of the General Counsel. (Mills Decl. ¶ 9.) There, a lawyer started a quick review of the retrieved files and saw a document appearing to be a communication by Hasselbring to a lawyer. (*Id.* ¶ 10.) The lawyer did not read the substance of the communication, and the Vanderbilt Legal Team was not told the contents of that communication. (*Id.* ¶¶ 10-11.) Vanderbilt's Legal Team informed Vanderbilt's Office of the General Counsel that no further review of the Hasselbring Backups should occur pending further

research as to whether a privilege attached to any documents in the Hasselbring Backups given Vanderbilt's Acceptable Use Policy and Notice to Users. (*Id.* ¶ 12.)

Although further legal research confirmed that Hasselbring had clearly waived any privilege that might otherwise attach to the documents in the Hasselbring Backups, the Vanderbilt Legal Team took steps to ensure that no lawyer on the team saw potentially privileged communications contained in the Hasselbring Backups. (*Id.* ¶ 13.) More specifically, Vanderbilt's Legal Team had the Bass, Berry & Sims Litigation Technology department, who are not lawyers, run searches on the data contained in the Hasselbring Backups to locate any potentially privileged communications. (*Id.* ¶ 14.) Those searches included the name of every lawyer that could be identified who was or had represented any defendant in this action. (*Id.*) Those searches identified 229 documents, and, because those documents were potentially privileged, the Litigation Technology department segregated those documents from the rest of the data comprising the Hasselbring Backups. (*Id.* ¶ 15; Gene L. Humphreys Decl. ¶ 6 (Exhibit C).) No member of the Vanderbilt Legal Team has had access to the 229 segregated documents. (Mills Decl. ¶ 16.) Following the segregation of those documents, an additional 578 documents (collectively, along with the 229 documents identified in the privilege screen, the "Documents") were flagged as potentially privileged by the Contract Reviewers while reviewing the documents on the Hasselbring Backups. (*Id.* ¶ 17.) The Vanderbilt Legal Team took great care to ensure that none of the Documents were shared with or reviewed by the Team. (*Id.* ¶ 22.)

Instead, Gene Humphreys, a senior member of Bass, Berry & Sims, served as an independent reviewer of the Documents. (*Id.* ¶ 18.) Mr. Humphreys is not a member of the Vanderbilt Legal Team, and his service as an independent reviewer has been his only involvement in this action. (*Id.* ¶¶ 18, 21; Humphreys Decl. ¶ 4.) Mr. Humphreys reviewed the Documents to

make a determination as to whether any of the Documents were arguably privileged on their face. (Mills Decl. ¶ 19.) He made that determination without consideration of Vanderbilt's Acceptable Use policy, the Notice to Users, or the storage of the Documents on Vanderbilt's systems. (*Id.*; Humphreys Decl. ¶ 11.) Prior to performing his review, Mr. Humphreys was advised not to discuss his review of the Documents with any member of the Vanderbilt Legal Team, and so he did not share the contents of the Documents with any member of the Vanderbilt Legal Team. (Mills Decl. ¶¶ 18-19.)

Of the 807 Documents reviewed, Mr. Humphreys identified 237 Documents that were arguably privileged on their face (*i.e.*, the Relevant Documents) and 570 Documents that were clearly not privileged. (Humphreys Decl. ¶¶ 12, 15.) Mr. Humphreys did not consider any of these 570 Documents to be privileged under any reasonable understanding of the attorney-client privilege, work-product doctrine, or accountant-client privilege. (*Id.* ¶ 15.) Of the 237 Relevant Documents, all were either emails or attachments to emails. (*Id.* ¶ 12.) More specifically, 85 Relevant Documents were arguably privileged under the attorney-client privilege or the work-product doctrine, with (i) 29 Relevant Documents were communications between Hasselbring and his counsel relating to this action where legal advice was being sought or given, or where facts relating to the action were being discussed; (ii) 12 Relevant Documents were communications between Hasselbring and an attorney but not related to this action; and (iii) 44 Relevant Documents were communications between Hasselbring and his counsel related to this action, but where no legal advice was sought or given and no facts relating to the action were discussed. (*Id.* ¶ 13.) The remainder 152 Relevant Documents were arguably privileged under the accountant-client privilege. (*Id.* ¶ 14.) These 237 Relevant Documents are the subject of this Motion. (Mills Decl. ¶ 23.)

PROCEDURAL BACKGROUND

On January 16, 2018, Vanderbilt filed its original complaint against Hasselbring and other defendants. (Compl. (Dkt. No. 1).) Vanderbilt amended its complaint against Hasselbring and those other defendants on August 31, 2018. (First Am. Compl. (Dkt. No. 85).) On September 25, 2018, the Court entered its initial case management order, setting discovery and other deadlines. (Dkt. No. 93.) Discovery between the parties has been ongoing since. On October 3, 2019, the Court amended its case management order, extending, among other deadlines, the close of fact discovery to December 20, 2019, and the deadline for discovery motions to December 4, 2019. (Dkt. No. 154.)

On September 17, 2019, counsel for Vanderbilt and counsel for Hasselbring had a telephone conference during which counsel for Vanderbilt informed Hasselbring's counsel of the circumstances of the Hasselbring Backups and the Relevant Documents and Vanderbilt's position that any privilege that might have otherwise attached to the Relevant Documents had been waived. On that call, Hasselbring's counsel asked to view all documents in the Hasselbring Backups. Vanderbilt's counsel declined to comply with this request, stating that, because no review of those documents had been performed by the Vanderbilt Legal Team, there was no basis to believe those documents were responsive to any discovery request and that those documents were the property of Vanderbilt. On September 18, Hasselbring's counsel sent a letter by email to Vanderbilt's counsel purporting to "clawback" all documents on the Hasselbring Backups.

On October 3, 2019, Vanderbilt's counsel shared with Hasselbring's counsel a letter summarizing Vanderbilt's position and inquired as to whether Hasselbring's counsel concurred that any privilege as to the Relevant Documents had been waived. Hasselbring's counsel did not agree, and the parties could reach no compromise on the issue. On October 25, Vanderbilt filed

the parties' Joint Statement regarding their dispute, in which Vanderbilt stated it planned to file a Motion for Protective Order. (Dkt. No. 159 (Exhibit D).) The Court stated it would await Vanderbilt's Motion before ruling on the parties' dispute. (Dkt. No. 161.)

CHOICE OF LAW

In cases relying on federal question jurisdiction, "questions of privilege are governed by federal common law." *Power & Tel. Supply Co. v. Suntrust Banks, Inc.*, No. 03-2217M1V, 2004 WL 784822, at *2 (W.D. Tenn. Feb. 17, 2004); *see also Reed v. Baxter*, 134 F.3d 351, 355 (6th Cir. 1998) ("Questions of privilege are to be determined by federal common law in federal question cases."). Likewise, "[w]here there are pendent state claims, federal common law still governs all claims of privilege." *Suntrust Banks*, 2004 WL 784822, at *2; *see also Hancock v. Dodson*, 958 F.2d 1367, 1373 (6th Cir. 1992) (stating that "in federal question cases where pendent state claims are raised the federal common law of privileges should govern all claims of privilege raised in the litigation"); *Coone v. Chattanooga-Hamilton Cty. Hosp. Auth.*, No. 1:16-CV-481, 2017 WL 9476830, at *1 (E.D. Tenn. May 18, 2017) ("It is well settled in the Sixth Circuit that, where a federal court exercises federal question jurisdiction, the federal (not state) law of privilege applies to the entire case. This is true even where there is a state law claim over which the federal court is exercising supplemental jurisdiction.").[1] Finally, "the work-product doctrine is a procedural rule of federal law," and, therefore, applies to all claims in both federal question and diversity jurisdiction cases. *In re Professionals Direct Ins. Co.*, 578 F.3d 432, 438 (6th Cir. 2009). Thus, federal law applies to the assertion of privilege and attorney work product (or the lack thereof) in this case.

[1] Because federal common law applies, the accountant-client privilege under Tennessee law, Tenn. Code § 62-1-116, is inapplicable. *See Hancock*, 958 F.2d at 1373. Nevertheless, out of an abundance of caution, Documents that could fall under the privilege were included in the Relevant Documents. In any event, the accountant-client privilege was waived. *See infra*.

ARGUMENT

Federal common law recognizes the attorney-client privilege. *See Suntrust Banks*, 2004 WL 784822, at *2. In the Sixth Circuit, the basic elements of the federal attorney-client privilege are:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection is waived.

Diamond Resorts Int'l, Inc. v. Phillips, No. 3:17-CV-01124, 2018 WL 3326814, at *2 (M.D. Tenn. Apr. 17, 2018) (quoting *Reed*, 134 F.3d at 355). Federal law likewise recognizes the work-product doctrine, or the work-product immunity, under Federal Rule of Civil Procedure 26(b)(3). *See Professionals Direct*, 578 F.3d at 438. Rule 26(b)(3) protects only (1) "documents and tangible things," (2) that are "prepared in anticipation of litigation or for trial" and (3) are "by or for another party or its representative." *Id.*

The attorney-client privilege under federal law "is narrowly construed because it reduces the amount of information discoverable during the course of a lawsuit." *In re Columbia/HCA Healthcare Corp.*, 192 F.R.D. 575, 577 (M.D. Tenn. 2000) (quoting *In re Grand Jury Proceedings October 12*, 1995, 78 F.3d 251, 254 (6th Cir. 1996)), *aff'd*, 293 F.3d 289 (6th Cir. 2002). In other words, the attorney-client privilege "is an exception carved from the rule requiring full disclosure, and as an exception should not be extended to accomplish more than its purpose." *Diamond Resorts*, 2018 WL 3326814, at *2 (quoting *United States v. Goldfarb*, 328 F.3d 280, 282 (6th Cir. 1964)). The work-product immunity is "broader than the attorney-client privilege," in that it covers "documents prepared by a lawyer in anticipation of litigation." *Reitz v. City of Mt. Juliet*, 680 F. Supp. 2d 888, 892 (M.D. Tenn. 2010).

Under federal law, the party asserting the attorney-client privilege has the burden of establishing its existence. *See Columbia/HCA*, 192 F.R.D. at 577. The party asserting the attorney-client privilege also has the burden to establish that the privilege has not been waived. *See Guy v. Yusen Logistics (Americas), Inc.*, No. 218CV02117MSNTMP, 2019 WL 2465173, at *6 (W.D. Tenn. Apr. 11, 2019) ("The burden of establishing that the privilege has not been waived falls on the party asserting the privilege."); *see also Edwards v. Whitaker*, 868 F. Supp. 226, 228 (M.D. Tenn. 1994) ("When a producing party claims inadvertent disclosure, it has the burden of proving that the disclosure was truly inadvertent and that the attorney/client privilege has not been waived."). For the work-product doctrine, courts apply a burden-shifting analysis. *See John B. v. Goetz*, 879 F. Supp. 2d 787, 896 (M.D. Tenn. 2010). As with the attorney-client privilege, the party asserting the work-product doctrine has the burden to establish that the doctrine has not been waived. *See Columbia/HCA*, 293 F.3d at 307. For purposes of this Motion, Hasselbring has the burden of establishing the non-waivers of both the attorney-client privilege and the work-product immunity.[2]

I. Any Attorney-Client Privilege or Work-Product Immunity Applicable to the Relevant Documents Has Been Waived by Hasselbring by His Use of Vanderbilt's Systems.

A waiver of the attorney-client privilege occurs "by voluntary disclosure of private communications by an individual or corporation to third parties." *United States v. Dakota*, 197 F.3d 821, 825 (6th Cir. 1999). "In addition, a client may waive the privilege by conduct which implies a waiver of the privilege or a consent to disclosure." *Id.* "The prevailing view is that once a client waives the privilege to one party, the privilege is waived en toto." *Columbia/HCA*, 293

[2] As noted *supra*, the accountant-client privilege is inapplicable, and even if it were not, Hasselbring also has the burden of establishing its non-waiver. *See First Horizon Nat'l Corp. v. Houston Cas. Co.*, No. 2:15-CV-2235-SHL-DKV, 2016 WL 5867268, at *8 (W.D. Tenn. Oct. 5, 2016).

F.3d at 294. When a waiver of the attorney-client privilege has been shown, a similar waiver of the work-product doctrine has been demonstrated. *See id.* at 306-07 ("[T]here is no compelling reason for differentiating waiver of work product from waiver of attorney-client privilege.").

To determine whether an employee has waived the attorney-client privilege through his use of his employer's technology systems, the four-factor analysis developed in *In re Asia Global Crossing Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005) applies. In *Asia Global*, the court considered "the analogous question of [an] employee's expectation of privacy in his office computer and the company e-mail system." *Id.* at 256. In doing so, the court equated an employee's reasonable expectation of privacy in company property – such as computer files and e-mails – with an employee's reasonable expectation that his personal communications using company property will remain confidential for attorney-client privilege purposes. *Id.* at 256-58; *see also Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (concluding that an employee had no reasonable expectation of privacy in workplace computer files where employer "had announced that it could inspect the laptops that it furnished for the use of its employees"); *Kelleher v. City of Reading*, No. Civ. A. 01–3386, 2002 WL 1067442, at *7-8 (E.D. Pa. May 29, 2002) (holding that an employee had "no reasonable expectation of privacy" in workplace e-mail where employer's guidelines "explicitly informed employees that there was no such expectation of privacy"). Therefore, to assess whether an employee has an expectation of privacy in his personal communications using company property, the court in *Asia Global* considered four factors:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

322 B.R. at 257.

Courts in the Sixth Circuit and elsewhere have since applied the four *Asia Global* factors to decide whether an employee's use of his employer's technology systems waived the attorney-client privilege. For example, the District Court for the Western District of Kentucky recently applied the *Asia Global* decision to conclude that employees had waived their attorney-client privilege as to emails with counsel "made via [the employer's] systems." *Pinnacle Sur. Servs., Inc. v. Manion Stigger, LLP*, 370 F. Supp. 3d 745, 754 (W.D. Ky. 2019). According to the *Pinnacle* Court, while the employer did not show that third parties had access to the employees' workplace emails, the employer had sufficiently demonstrated the other three *Asia Global* factors to show the employees had waived their attorney-client privilege. First, the Court observed that the employer "prohibited" unauthorized "use of its systems." *Id.* at 753. Second, the employer's policies stated that the employer "monitored its employees' use of its systems." *Id.* Third, the employees were aware of the employer's policies having received a copy of them. *Id.* For those reasons, the District Court for the Western District of Kentucky concluded that the employees had waived the attorney-client privilege as to their communications with counsel "made via [the employer's] system." *Id.* at 754.

As the *Pinnacle* decision demonstrates, where an employer articulates a policy limiting or otherwise restricting employees' use of its system while notifying employees of its policy, and the employee uses the system, the employee has waived the attorney-client privilege by his use of that system. *See Bingham v. Baycare Health Sys.*, No. 8:14-CV-73-T-23JSS, 2016 WL 3917513, at *5 (M.D. Fla. July 20, 2016) (concluding that, under *Asia Global*, an employee's workplace emails and attachments were not privileged because the employee "did not have a reasonable expectation of confidentiality in his workplace e-mails" given the employer's clear policy limiting use of its system and reserving the employer's right to monitor and access computers); *Long v. Marubeni*

Am. Corp., No. 05CIV.639(GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (stating that, because employees "knew or should have known of [employer's]" policy informing employees of email monitoring and prohibiting personal use, the employees' communications to attorneys using the employer's computer system were not protected by attorney-client privilege); *In re Royce Homes, LP*, 449 B.R. 709, 732-33 (Bankr. S.D. Tex. 2011) (concluding that an employee "waived the attorney-client privilege as to any e-mails he sent and received via the [employer's] computer system, as any communications between [the employee] and his personal counsel were not confidential" because of the employer's policy prohibiting personal use and warning of monitoring personal communications on its server); *In re Info. Mgmt. Servs., Inc. Derivative Litig.*, 81 A.3d 278, 286-92 (Del. Ch. 2013) (applying the four-factor test from *Asia Global* to conclude that the attorney-client privilege did not apply to employees' emails and attachments given employer's policy and employee's awareness of policy).

Applying *Asia Global* here, Hasselbring's use of Vanderbilt's systems waived any attorney-client privilege as to the Relevant Documents. The first *Asia Global* factor asks "does the [employer] maintain a policy banning personal or other objectionable use." 322 B.R. at 257. Vanderbilt's Acceptable Use Policy clearly informs users of appropriate computer use, stating that Vanderbilt's systems should only be used for their "intended purposes," and warns about the consequences of misuse. (Sidiqyar Decl. ¶ 3, Exhibit 1); *see also Bingham*, 2016 WL 3917513, at *4 ("[T]he majority of courts have found that an employee has no reasonable expectation of privacy in workplace e-mails when the employer's policy limits personal use or otherwise restricts employees' use of its system and notifies employees of its policy."). Likewise, the Notice to Users prompt appearing on employees' screens before entering Vanderbilt's systems states, "Unauthorized or improper use of this system may result in civil and/or criminal penalties and

administrative or disciplinary action." (Sidiqyar Decl. ¶ 14, Exhibit 2); *see also Royce Homes*, 449 B.R. at 738 (noting that policy warning prohibiting "certain computer uses," including profanity and sexual harassment, was sufficient to satisfy first *Asia Global* factor). Moreover, Vanderbilt's Acceptable Use Policy expressly cautions users that they "should not expect that records created, stored or communicated with Vanderbilt information technology or in the conduct of Vanderbilt's business will necessarily be private." (Sidiqyar Decl. ¶ 3, Exhibit 1.) The Notice to Users is even more explicit, stating "USERS (AUTHORIZED OR UNAUTHORIZED) HAVE NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY." (Sidiqyar Decl. ¶ 14, Exhibit 2); *see also Pinnacle*, 370 F. Supp. 3d at 753 (observing that the first *Asia Global* factor was satisfied where the policy warned "[e]mployees should have no expectation of privacy of any correspondence, messages or information in the systems"); *United States v. Angevine*, 281 F.3d 1130, 1132 (10th Cir. 2002) (holding, in a criminal proceeding, that a professor had no reasonable expectation of privacy in university computer and its files where a university's computer policy "explain[ed] appropriate use, warn[ed] employees about the consequences of misuse, and describe[d] how officials administer and monitor the University computer network"). Vanderbilt's IT policies satisfy the first *Asia Global* factor.

Second, the next *Asia Global* factor inquires as to whether "the [employer] monitor[s] the use of the employee's computer or e-mail." 322 B.R. at 257. Vanderbilt has the ability to and warns in its IT policies that it may monitor computer use or transactions. Vanderbilt's Acceptable Use Policy warns users that "Vanderbilt uses automated systems to monitor data transmissions entering and leaving the Vanderbilt networks to detect the presence of viruses, malicious software, or privileged information." (Sidiqyar Decl. ¶ 3, Exhibit 1); *see also Long*, 2006 WL 2998671, at *3 (finding *Asia Global*'s second factor sufficiently demonstrated where employer's policy stated

that the employer "had the right to monitor all data flowing through its automated systems"). The Notice to Users similarly informs users that "all uses of" and "all data on" Vanderbilt's systems "may be *intercepted*, *monitored*, *recorded*, copied, audited, inspected, and disclosed to your employer." (Sidiqyar Decl. ¶ 14, Exhibit 2 (emphasis added).) The statement in the Notice to Users that users have "NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY" further underscores that users expected and, in fact, consented to Vanderbilt's monitoring. (*Id.*; *see also Id.* ¶ 3, Exhibit 1 (warning that users "should not expect" that their communications "will necessarily be private")); *Royce Homes*, 449 B.R. at 739 (concluding that the second *Asia Global* was satisfied because of employer's policy warning that "nothing on [any electronic system] will be considered private"). Vanderbilt's IT policies satisfy the second *Asia Global* factor.

Third, *Asia Global* asks "do third parties have a right of access to the computer or e-mails." 322 B.R. at 257. As an initial matter, Vanderbilt – a third party vis-à-vis Hasselbring and his counsel – had access to the Vanderbilt-owned computers issued to Hasselbring. *See Bingham*, 2016 WL 3917513, at *5 (concluding the third *Asia Global* factor was met where the employer "reserved the right to access, read, and disclose any electronic communication sent or received over its communications systems"); *Info. Mgmt. Servs.*, 81 A.3d at 290-91 (observing that "by definition the employer has the technical ability to access the employee's work email account" and finding the third *Asia Global* factor satisfied because the employer, "a third party to the communication, had the right to access [the employees'] emails when they communicated using their work accounts"). Moreover, Vanderbilt's Acceptable Use Policy allowed for others to inspect the data, including email, on the computer used by Hasselbring when necessary, stating that compliance requirements or investigations "may require observation of electronic information by … authorized agents" beyond Vanderbilt employees and officials. (Sidiqyar Decl. ¶ 3, Exhibit

1.) The Notice to Users provided users with a similar warning: "Any or all uses of [Vanderbilt's systems] and all data on [Vanderbilt's systems] may be intercepted, monitored, *recorded*, *copied*, *audited*, *inspected*, and disclosed to your employer." (*Id.* ¶ 14, Exhibit 2 (emphasis added).) Vanderbilt's policies, therefore, allowed third parties a right of access to the computers and email used by Hasselbring.

Finally, the last *Asia Global* factor examines whether the employer "notif[ied] the employee, or was the employee aware, of the use and monitoring policies." 322 B.R. at 257. Vanderbilt made Hasselbring aware of its policies, and Hasselbring was, in fact, aware of them. Vanderbilt's Acceptable Use Policy, which was included in the Faculty Manual and made available to Hasselbring, states:

> All members of the Vanderbilt University community are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All users are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of the University's IT resources.

(Sidiqyar Decl. ¶ 3, Exhibit 1.) This notice satisfies the fourth *Asia Global* factor because an employer must simply make its employees aware of its policy to meet this factor. *See Bingham*, 2016 WL 3917513, at *5 (stating the fourth factor was met because employer "made its employees, including Plaintiff, aware of its policy"). Given Hasselbring's decades-long employment with Vanderbilt, Hasselbring cannot now claim unawareness of Vanderbilt's policies. (First Am. Compl. ¶¶ 17-19.) In any event, Hasselbring *has admitted* in this litigation that the Faculty Manual containing the Acceptable Use Policy was part of his contractual relationship with Vanderbilt. (Dkt. No. 129 ¶ 19; *see also id.* ¶ 7, Counterclaim (alleging that the Faculty Manual was an enforceable part of his employment agreement).)

Moreover, the Notice to Users requires users to click "Proceed" before using Vanderbilt's systems but warns that "BY CONTINUING TO USE [Vanderbilt's systems] YOU INDICATE YOUR AWARENESS AND CONSENT TO THESE TERMS AND CONDITIONS OF USE." (Sidiqyar Decl. ¶ 14, Exhibit 2.) If a user does not consent, the Notice of Users instructs the users to log off immediately. (*Id.*) Hasselbring, therefore, had to affirm that he was aware of and consented to Vanderbilt's policies before entering its systems and, in fact, consented to Vanderbilt's IT policies ***at least*** twelve times.[3] (*Id.* ¶ 19.)

***

Given Vanderbilt's policies and Vanderbilt's notification to Hasselbring making him aware of those policies, Hasselbring's use of Vanderbilt's systems when communicating with counsel waived the attorney-client privilege, and consequently the work-product immunity, as to the Relevant Documents.[4]

II. The Relevant Documents Were Not Inadvertently Disclosed.

Under certain circumstances, an inadvertent disclosure of privileged information "made in a federal proceeding" will "not operate as a waiver." Fed. R. Evid. 502(b); (*see also* Dkt. No. 105 (Protective Order)). Federal Rule of Evidence 502(b) provides that a disclosure of privileged information will not operate as a waiver only when (1) the disclosure was "inadvertent," (2) "the holder of the privilege or protection took reasonable steps to prevent disclosure," and (3) "the holder promptly took reasonable steps to rectify the error." Fed. R. Evid. 502(b); *see also Inhalation Plastics, Inc. v. Medex Cardio-Pulmonary, Inc.*, No. 2:07-CV-116, 2012 WL 3731483,

[3] Regardless, "actual or direct notification to employees is unnecessary if the corporation has a communications policy that is memorialized." *Royce Homes*, 449 B.R. at 741. Vanderbilt's Acceptable Use Policy is unquestionably memorialized. (Sidiqyar Decl. ¶ 3, Exhibit 1.)

[4] This conclusion applies with equal force to the accountant-client privilege.

at *3 (S.D. Ohio Aug. 28, 2012). Hasselbring's use of Vanderbilt's systems when communicating with counsel did not cause any inadvertent disclosure because Vanderbilt's possession of the Relevant Documents occurred through neither inadvertence nor a disclosure in a federal proceeding.

A. Vanderbilt's Possession of the Relevant Documents Was Not the Result of Inadvertence.

For Federal Rule of Evidence 502(b) to apply, a "disclosure" must be "inadvertent." A voluntary disclosure, however, is not "inadvertent" and waives the attorney-client privilege. *Dakota*, 197 F.3d at 825; *see also N. Am. Rescue Prod., Inc. v. Bound Tree Med., LLC*, No. 2:08-CV-101, 2009 WL 4110889, at *9 (S.D. Ohio Nov. 19, 2009) ("A party waives the attorney-client privilege notwithstanding an error of judgment where the person knows that privileged information is being released but concludes that the privilege will nevertheless survive." (quoting *Maday v. Public Libraries of Saginaw*, 480 F.3d 815, 821 (6th Cir. 2007))).

Vanderbilt's possession of the Relevant Documents did not come about through Hasselbring's inadvertence. Rather, Vanderbilt gained possession of the Relevant Documents through Hasselbring's voluntary, intentional, and repeated use of Vanderbilt's systems. *See Long*, 2006 WL 2998671, at *4 (observing that, under Federal Rule of Evidence 502(b), employees' disclosure was not inadvertent because the employees "did not use their [employer] assigned computers and their [employer] provided internet access accidentally or inadvertently to exchange the pertinent e-mail messages; they did so voluntarily, intentionally and repeatedly"). Vanderbilt made clear through its Acceptable Use Policy, which was, again, included in the Faculty Manual and made available to Hasselbring, that Hasselbring's use of Vanderbilt's systems revealed his data and communications to Vanderbilt. (Sidiqyar Decl. ¶ 3, Exhibit 1.) And this was made even more clear the twelve times Hasselbring accessed Vanderbilt's system through the Vanderbilt VPN

and received the "Notice to Users" prompt, which clearly warned him that "all uses of" and "all data on" Vanderbilt's systems "may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to your employer." (*Id.* ¶ 14, Exhibit 2.) The Notice to Users further stated that Vanderbilt considered use of its systems as "consent to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of such personnel or officials." (*Id.*) Finally, in all capital letters, the Notice to Users warned users that "BY CONTINUING TO USE [Vanderbilt's systems] YOU INDICATE YOUR AWARENESS AND CONSENT TO THESE TERMS AND CONDITIONS OF USE" and that they should log off immediately if they do not consent. (*Id.*) The Notice to Users required users to click "Proceed" before using Vanderbilt's systems. (*Id.*) With those warnings, Hasselbring accessed Vanderbilt's network twelve times. (*Id.* ¶ 19.) In short, Hasselbring's use of Vanderbilt's system was neither accidental nor inadvertent; it was intentional and voluntary. *See Long*, 2006 WL 2998671, at *4; *Centennial Bank v. Servisfirst Bank Inc.*, No. 816MC00082CEHJSS, 2016 WL 6037552, at *9-10 (M.D. Fla. Oct. 14, 2016) (concluding that email communications with attorney sent through a workplace email account were not inadvertently disclosed where employer had policy warning of potential email monitoring).

The conclusion that Hasselbring's use of Vanderbilt's systems was not "inadvertent" under Federal Rule of Evidence 502(b) aligns with the American Bar Association's ("ABA") analogous conclusion regarding Model Rule of Professional Conduct 4.4(b). Under Rule 4.4(b), "[a] lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender." Applying that language, the ABA concluded, "[E]-mails between an employee and his or her counsel are not 'inadvertently

sent' by either of them." (ABA Formal Op. 99-413 (Exhibit E).) The ABA reached that conclusion reasoning:

> A 'document [is] inadvertently sent' to someone when it is accidentally transmitted to an unintended recipient, as occurs when an e-mail or letter is misaddressed or when a document is accidentally attached to an e-mail or accidentally included among other documents produced in discovery. ***But a document is not 'inadvertently sent' when it is retrieved by a third person from a public or private place where it is stored or left.***

(*Id.* (emphasis added).) Therefore, according to the ABA, where an employee uses his employer's system to send email communications with counsel, the employer's receipt of those communications did not occur through the employee's "inadvertent" disclosure.

Here, Hasselbring willingly accepted that Vanderbilt would monitor his use and access his data while on its systems, and he did so even after repeatedly receiving Vanderbilt's unambiguous warning regarding its policies. As a result, Hasselbring's use of Vanderbilt's systems was not inadvertent, but rather voluntary and intentional. *Long*, 2006 WL 2998671, at *4. Therefore, no inadvertent disclosure of the Relevant Documents occurred here, and Federal Rule of Evidence 502(b) is inapplicable.

B. No Disclosure Was Made in a Federal Proceeding.

For Federal Rule of Evidence 502(b) to apply, a "disclosure" must have been "made in a federal proceeding." No such disclosure occurred here.

First, Hasselbring made no "disclosure" of the Relevant Documents under Federal Rule of Evidence 502(b). Vanderbilt actually discovered the emails; the Relevant Documents were not disclosed by Hasselbring. (Mills Decl. ¶¶ 8-9.) When an employer discovers employee emails on its systems, that discovery is not a "disclosure" for purposes of Federal Rule of Evidence 502(b). *See Long*, 2006 WL 2998671, at *4 ("Here, the [employees] did not 'disclose' the e-mail messages to the defendants during the pretrial discovery phase of the litigation. Rather, [the employer]

discovered these communications while reviewing [the employer's] computers to fulfill [the employer's] disclosure obligations in this litigation and, thereafter, 'disclosed' them to the [employees]."). As no disclosure of the Relevant Documents occurred here, Federal Rule of Evidence 502(b) does not apply.

Second, even assuming a "disclosure" occurred, that disclosure was not "made in a federal proceeding" as required under Federal Rule of Evidence 502(b). *See id.* at *4 (holding that documents were not disclosed "in a federal proceeding" but rather simply discovered while employer reviewed computers to fulfill its litigation disclosure obligations). Disclosures falling under the purview of Federal Rule of Evidence 502(b) must be made in a federal proceeding, as that rule focuses on inadvertent disclosures in the *production* of documents during litigation. *See* Fed. R. Evid. 502 (noting that the inadvertent disclosure rule applies when the disclosure is "made in a federal proceeding"). Here, any disclosure by Hasselbring was not made in a federal proceeding. Warned that Vanderbilt monitored its systems and that users should not expect their communications on the system to be private, Hasselbring accessed Vanderbilt's systems. Because of Hasselbring's use of Vanderbilt's system, Vanderbilt came into possession of the Relevant Documents. (Mills Decl. ¶¶ 8-9.) None of the Relevant Documents were disclosed through production during discovery. *See Pinnacle*, 370 F. Supp. 3d at 751.

Because Hasselbring did not make any "disclosure … in a federal proceeding," Federal Rule of Evidence 502(b) does not apply.

CONCLUSION

For the foregoing reasons, Hasselbring has waived any applicable privilege regarding the Relevant Documents. Accordingly, Vanderbilt requests that the Court grant its Motion for Protective Order and enter an Order ruling that the Relevant Documents are not privileged.

Respectfully submitted,

/s/ Paige W. Mills
Paige W. Mills #016218
Mary Leigh Pirtle #026659
Ashleigh Karnell #036074
Bass, Berry & Sims PLC
150 Third Avenue South, Suite 2800
Nashville, TN 37201
(615) 742-6200
pmills@bassberry.com
mpirtle@bassberry.com
ashleigh.karnell@bassberry.com

Attorneys for Plaintiff Vanderbilt University

CERTIFICATE OF SERVICE

I certify that a true and exact copy of the foregoing has been served upon these individuals, via the Court's CM/ECF e-mail notification system, on this the 8th day of November, 2019:

Caren Decter (*pro hac vice*)
Edward H. Rosenthal (*pro hac vice*)
Matt Woleske (*pro hac vice*)
Viviane Scott (*pro hac vice*)
Frankfurt, Kurnit, Klein & Selz, P.C
488 Madison Avenue
New York, NY 10022
(212) 826-5524
cdecter@fkks.com
erosenthal@fkks.com
mwoleske@fkks.com
vscott@fkks.com

Attorneys for Defendant, Scholastic Inc.

Thor Y. Urness, #13641
Bradley Arant Boult Cummings LLP
1600 Division Street
Suite 700
Nashville, TN 37203-0025
(615) 244-2582
turness@babc.com

Attorney for Defendant, Scholastic Inc.

Aubrey B. Harwell, Jr., #2559
Thomas H. Dundon, #4539
Erik C. Lybeck, #35233
Neal & Harwell, PLC
1201 Demonbreun Street
Suite 1000
Nashville, TN 37203
(615) 244-1713
aharwell@nealharwell.com
tdundon@nealharwell.com
elybeck@nealharwell.com

Attorneys for Defendant, Ted S. Hasselbring

Benjamin E. Marks (*pro hac vice*)
David J. Lender (*pro hac vice*)
Jessica Falk (*pro hac vice*)
Sara Lonks (*pro hac vice*)
Taylor Dougherty
Weil, Gotshal & Manges
767 Fifth Avenue
New York, NY 10153
(212) 310-8000
benjamin.marks@weil.com
david.lender@weil.com
jessica.falk@weil.com

Attorneys for Defendant, Houghton Mifflin Harcourt Publishing Company

Michael G. Abelow, #26710
Sherrard Roe Voight & Harbison, PLC
150 Third Avenue South
Suite 1100
Nashville, TN 37201
(615) 742-4532
mabelow@srvhlaw.com

Attorney for Defendant, Houghton Mifflin Harcourt Publishing Company

/s/ Paige W. Mills